

JMM:SK  
F.#2013R00948

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

- - - - - X

UNITED STATES OF AMERICA

- against -

**DECLARATION OF  
OVIE CARROLL**

PHILLIP A. KENNER and  
TOMMY C. CONSTANTINE,  
also known as  
“Tommy C. Hormovitis,”

Defendants.

- - - - - X

I, Ovie Carroll, declare:

1. I am employed by the U.S. Department of Justice (“DOJ”). I am currently the Director for the DOJ CyberCrime Lab at the Computer Crime and Intellectual Property Section and a Digital Forensics Certified Examiner. The CyberCrime Lab provides advanced computer forensics, and cybercrime investigative and other technical support to DOJ prosecutors as it applies to implementing the Department’s national strategies in digital evidence, combating electronic penetrations, data thefts, and cyber attacks on critical information systems.

2. I am also an adjunct professor with George Washington University and teach a class on CyberCrime/Internet Investigations in the Masters of Forensic Science program. I am also a course author and instructor with the SANS Institute where I teach Digital Forensics.

3. Prior to joining the DOJ, I was the Special Agent in Charge of the Technical Crimes Unit at the United States Postal Service, Office of Inspector General, responsible for all computer intrusion investigations within the Postal Service network infrastructure and for providing all digital forensic analysis in support of criminal investigations and audits.

4. I have also previously served as the Special Agent in Charge of the Computer Investigations and Operations Branch at the Air Force Office of Special Investigations, responsible for coordinating all national level computer intrusions occurring within the United States Air Force.

5. My curriculum vitae is attached hereto as Exhibit A.

6. Based on my training and experience, I have gained expertise in the forensic analysis of computers, cellular telephones, and other digital media.

7. Digital forensic analysis involves the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for law enforcement purposes.

8. During the digital forensic analysis process for computers, a forensic examiner images the hard drive of the original computer to create a copy of the original (the "imaged copy"). The forensic examiner then proceeds with the digital forensic analysis process using the imaged copy.

9. It is not the routine practice of forensic examiners to thereafter power up the original computer. This is not the routine practice so that the original hard drive is not altered, manipulated, or damaged in any way.

10. Powering up the original computer will typically alter the data on the hard drive of the original computer. For example, powering up the original computer may overwrite files that existed on the original hard drive in unallocated space. This is because during a typical startup or boot process of a computer system, hundreds of files will be accessed and may be written into temporary storage space on the hard drive and that temporary storage space, also known as “unallocated space,” may contain files that were previously deleted (a file that is deleted on a computer system typically remains in unallocated space until overwritten). In addition, powering up the original computer may alter the metadata of files that existed on the original hard drive (for example, the last-accessed date and time of an operating system file). Moreover, powering up the original computer may change the computer system’s audit logs and last known configuration parameters that existed on the original hard drive, including information regarding the last known users and networks.

11. A forensic examiner may make the contents of a computer available for inspection in the following manner: (i) an imaged copy may be connected to a standalone computer, which would permit the inspection of files in the imaged copy; (ii) an imaged copy may be restored to a standalone hard drive and booted to a computer, which would permit the inspection of files as they appeared on the original computer.

12. Similarly, it is not the routine practice of forensic examiners to power up an original cellular telephone after it has been imaged. Powering up an original cellular telephone will typically alter the data on the cellular telephone; for example, it may overwrite files, alter metadata, or change audit logs.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on November 3, 2014.

A handwritten signature in black ink, appearing to read "O. Carroll", written over a horizontal line.

Ovie Carroll  
Director, CyberCrime Lab  
U.S. Department of Justice

# **EXHIBIT A**

# OVIE CARROLL

## DIRECTOR OF THE CYBERCRIME LABORATORY COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION

1301 NEW YORK AVE NW, WASHINGTON, DC 20005  
OVIE.CARROLL@USDOJ.GOV  
202-514-1026

### SUMMARY OF EXPERIENCE

Accomplished professional with over 28 years of experience in implementing innovative solutions in cybercrime and criminal investigations, digital investigative analysis (computer forensics), security and safety policies, procedures, and standards that balance the needs of public safety and privacy in cyberspace.

- ❖ Demonstrated ability to investigate complex cybercrime matters, gather and analyze pertinent digital evidence, and resolve investigative matters.
- ❖ Exemplified in-depth knowledge and expertise in digital forensics and investigative techniques in technology-driven environments.
- ❖ Recognized for upholding a positive attitude, work effort, and professional ethics and standards.
- ❖ Certified Digital Forensics Examiner, George Washington University Adjunct Professor, and Co-author of SANS Institute Forensics 408 Windows In Depth.

### AREAS OF EXPERTISE

Cybercrime Investigation/Incident Response  
Digital Investigative Analysis  
Computer Forensic Training and Development  
Computer Intrusion Investigation Management  
Digital Forensic Research and Development  
Performance Management  
Public Speaking

### PROFESSIONAL EXPERIENCE

DIRECTOR OF THE CYBERCRIME LABORATORY  
Computer Crime and Intellectual Property Section  
Department of Justice – Criminal Division  
Washington, DC 20530

2006–Present

- Manage direct reports while serving as the primary technical advisor to senior Department of Justice officials on digital forensics and cybercrime fighting techniques; provide technical and investigative advice on matters involving complex computer security, digital evidence, and critical infrastructure issues.

OVIE CARROLL

- Analyze digital evidence, research and develop new digital forensics and cybercrime investigative techniques, and ensure availability of the highest quality digital evidence to prosecutors.
- Assist and support law enforcement and intelligence agencies in investigating matters of highly sensitive, complex, and difficult natures of cases, including Internet attacks and cyberspace communication characterized with obscure leads, few visible records, and conflicting evidence.
- Create, develop, and implement digital forensic, cybercrime crime, and online investigative programs within the Computer Crime and Intellectual Property Section; recommend upgrades in the area of non-standard hardware, software applications, and state-of-the-art technology innovations.
- Provide guidance to lawyers in the preparation of case material on computer forensics and other electronically stored information (ESI), as well as in locating pertinent and expert witnesses for trial.
- Lead training and provide consultation to federal law enforcement and other audiences relating to digital forensics, cybercrime investigations, network vulnerabilities, common network attacks, security procedures, and other computer issues.
- Coordinate and assist the department on cyber-infrastructure protection and in combating cyber-terrorism.
- Work with technologists in the private sector in solving and anticipating specific investigative problems, as well as in representing and promoting public safety interests in product development.

#### KEY ACCOMPLISHMENTS

- Recognized and trusted technical expert by the Federal Judicial Training Center for providing training to federal judiciary.
- Provided trainings on computer forensics and other cybercrime fighting techniques and capabilities to more than 400 magistrate judges in the United States.
- Played a pivotal role in evaluating and delivering the substantial needs of the Department of Justice Prosecutors in the areas of developing training programs and courses, such as the Computer Forensics for Prosecutors and Complex Online Crimes Investigations — recognized as the most requested course taught at the National Advocacy Center, the Department of Justice' training facility.
- Designed, equipped, and maintained the Department of Justice Cybercrime Computer Laboratory at the Computer Crime and Intellectual Property Section (CCIPS).
- Conducted extensive training to the Thailand Supreme Court and numerous federal prosecutors, judges, and law enforcers in different countries, including Singapore, South Africa, Malaysia, Mexico, Philippines, Moldavia, Thailand, Romania, Vietnam, South Korea and Brazil.

**ADJUNCT PROFESSOR**  
**Master of Forensic Science Program Course**  
**George Washington University**  
 Washington, DC 20052

2006–Present

OVIE CARROLL

- Adjunct Professor at George Washington University providing course curriculum instruction for the Master of Forensic Science Program, "Internet Investigations" and "Investigative Interviewing Techniques"

**Co-AUTHOR/CERTIFIED INSTRUCTOR**

2006–Present

**SANS****Forensics 408-Windows In-Depth**

Washington, DC 20052

- 
- Co-Author of Forensics 408-Windows In-Depth providing course curriculum instruction for advanced Windows digital investigative analysis.

**SPECIAL AGENT IN CHARGE**

2000–2006

**Technical Crimes Unit****Postal Inspector General's Office**

Arlington, VA 22209

- 
- Planned, developed, implemented, and managed criminal investigations into computer networks and examination of computer evidence obtained through the application of innovative incident response techniques.
  - Facilitated and coordinated multi-national investigations and analyzed all collaborated evidence in pursuit of criminal prosecution.

**CREDENTIALS**

- 
- 
- Top Secret, Sensitive Compartmented Information Security Clearance
  - Certified Nuix Forensic Analyst
  - Digital Forensics Certified Examiner
  - Certified UNIX System Administrator Professional | Learning Tree International
  - System Forensics, Investigations, and Response | Sans Institute
  - Certified Professional — UNIX Tools | Learning Tree International
  - Member, Scientific Working Group on Digital Evidence (SWGDE)

**PROFESSIONAL TRAINING**

- 
- 
- SANS MAC Forensic Analysis
  - Nuix Investigation Specialist
  - Autopsy Computer Forensic Program, Open Source Forensic Conference
  - Seized Computer and Evidence Recovery Specialist, FLETC
  - Computer Information Systems Security Professional (CISSP) Fast Track
  - EnCase Intermediate Forensic Examiners Course, Guidance
  - Forensic Tool Kit Intermediate Computer Forensics, Access Data

OVIE CARROLL

- Forensic Data Imaging, New Technologies, Inc.
- System Forensics, Investigations, and Response, Sans Institute Track 8
- Certified Professional, Unix System, Learning Tree International
- Certified Professional, Unix Tools, Learning Tree International
- Advanced Networking & System Security Exploitation
- Networking for Agents & System Security Exploitation, Sytex Inc.
- Computer Forensic Field Examiners Course, AFOSI

#### PUBLICATIONS & SPEAKING ENGAGEMENTS (SELECTED)

- Presenter – Tools to Protect Your Digital Data, North Texas Crime Commission, Oct 2014.
- Keynote - Cybercrime & Cyber Security, AFOSIA Convention, Sep 2014
- “Using Digital Fingerprints (or Hash Values) for Investigations and Cases Involving Digital Evidence”, United States Attorney Bulletin (DOJ Publication) May 2014.
- “SANS Forensics 408: Windows In-Depth” Current Training Program 2008-Present.
- Presenter - National Bar Association Judicial Council on Cyber Security and Ethics for Judges, July 2014
- Presenter – What Facebook and Google Known About You, Federal Judicial Center's Magistrate Judges Workshop, April & June 2014
- Presenter – Computer Forensics for Anti-Trust Investigations, Romanian Anti-Trust Crime Commission, May 2014
- “Computer Forensics: Digital Forensic Analysis Methodology”, United States Attorney Bulletin (DOJ Publication) January 2008.
- “Vista and Bit Locker and Forensics! Oh My!”, United States Attorney Bulletin (DOJ Publication) January 2008.
- “Managing Large Amounts of Electronic Evidence”, United States Attorney Bulletin (DOJ Publication) January 2008.
- “Rethinking the Storage of Computer Evidence”, United States Attorney Bulletin (DOJ Publication) January 2008.

#### AWARDS AND RECOGNITIONS

- Department of Justice Performance Award
- Assistant Attorney General's Award for Outstanding Litigation Support (2008)
- Directors Appreciation Award, Executive Office for U.S. Attorneys and the U.S. Attorney's Office (2008)
- Fellowship Award, The Institute of Computer Forensic Professionals (2008)